

## UNITED STATES DISTRICT COURT



for the

Western District of Washington

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)A Digital Forensic Image of the [REDACTED]  
cellular telephone, IMEI number [REDACTED], as  
further described in Attachment A

Case No. MJ21-566

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

A Digital Forensic Image of the Samsung Galaxy S8+ cellular telephone, IMEI number 352805090131463, as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Title 18, U.S.C. §§ 641, 1341, 1343,  
and 1028A

Offense Description

Theft of Public Funds, Mail Fraud, Wire Fraud, and Aggravated Identity  
Theft

The application is based on these facts:

- ☒ See attached Affidavit continued on the attached sheet

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.

Robert C. Patterson

Applicant's signature

Special Agent Robert C. Patterson, DHS-ICE

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or  
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 10/22/2021

Judge's signature

City and state: Seattle, Washington

Michelle L. Peterson, United States Magistrate Judge

Printed name and title



**INTRODUCTION AND PURPOSE OF AFFIDAVIT**

3. This affidavit is made in support of a search warrant for the digital forensic image ( "SUBJECT FORENSIC IMAGE") obtained from the cellular phone seized during the execution of an anticipatory search warrant of the premises of [REDACTED], Marysville, Washington 98270 (the "SUBJECT PREMISES") on February 23, 2021, for evidence of violations of Title 18, United States Code, Sections 641 (Theft of Public Funds), 1341 (Mail Fraud), 1343 (Wire Fraud), 1028A (Aggravated Identity Theft), and conspiracy to commit these offenses ("SUBJECT OFFENSES"). The SUBJECT FORENSIC IMAGE is in the custody of federal law enforcement agencies and is more fully described in Attachment A to the search warrant.

4. The items to be seized are evidence, fruits, and instrumentalities of violations of the SUBJECT OFFENSES. The items to be seized are listed in Attachment B to the search warrant.

**SUMMARY OF PROBABLE CAUSE**

5. *Search Warrant for Counterfeit Offenses.* On February 22, 2021, the Honorable Brian A. Tsuchida, granted an application for a search warrant for the address [REDACTED], Marysville, Washington 98270 (the "SUBJECT PREMISES") for evidence, fruits, and instrumentalities of violations of 18 U.S.C. 472 (Passing Counterfeit) and 473 (Dealing in Counterfeit) ("Search Warrant MJ21-101"). On February 23, 2021, agents and taskforce officers with ICE-HSI, the United States Secret Service ("USSS"), with assistance from Customs and Border Protection and the Marysville Police Department, conducted a controlled delivery operation of a seized DHL parcel containing counterfeit U.S. currency and executed the search warrant on the SUBJECT PREMISES.

6. During the search of the SUBJECT PREMISES, agents discovered and seized a Samsung cellular phone, which [REDACTED] acknowledged belonged to him. A forensic image of the Samsung cellular phone was made by Marysville Police Detective P. McShane and provided to me on March 3, 2021. The SUBJECT

1 FORENSIC IMAGE remains in the possession of the government who have begun to  
2 search it pursuant the list of items to be seized in Attachment B of Search Warrant MJ21-  
3 101. The Samsung cellular phone was returned to [REDACTED] in March 2021.

4 7. During execution of Search Warrant MJ21-101, agents discovered and  
5 seized various documents from the SUBJECT PREMISES, including checks from the  
6 Commonwealth of Pennsylvania payable to two individuals, [REDACTED]  
7 [REDACTED], both addressed to the SUBJECT PREMISES. Additionally, an opened envelope  
8 with a return address of the "Pennsylvania Treasury" in Harrisburg, Pennsylvania was  
9 discovered.

10 8. Agents discovered and seized approximately 25 photocopied and original  
11 MoneyGram receipts, in amounts ranging from \$210 to \$1,000, each payable to "PA UC  
12 Fund" with an address in Harrisburg, Pennsylvania. Agents also discovered and seized  
13 photocopies of three manila envelopes affixed with postage stamps, each addressed to the  
14 "PA UC Fund, The Department of Labor and Industry" in Harrisburg, Pennsylvania. One  
15 of the manila envelopes had a return addressee of [REDACTED] at the SUBJECT  
16 PREMISES, another with [REDACTED] at the SUBJECT PREMISES, and the third of  
17 [REDACTED] at the SUBJECT PREMISES.

18 9. Upon discovery of these documents, agents provided this information to  
19 USSS Special Agent Jack Richards who was conducting a consensual interview of Faisal  
20 SHEIKH in a government vehicle parked outside the SUBJECT PREMISES.

21 10. Special Agent Richards asked [REDACTED] about the checks from  
22 Pennsylvania. [REDACTED] responded by stating he and his wife, [REDACTED], had  
23 attempted to apply for Washington State unemployment benefits but her application was  
24 rejected. He stated he heard that Pennsylvania would pay him unemployment benefits.  
25 He then worked with a friend in Minnesota named [REDACTED], who told [REDACTED] to use  
26 [REDACTED]'s father's and sister's information to apply for unemployment benefits from  
27 Pennsylvania. [REDACTED] told [REDACTED] that these two individuals live in Virginia.  
28 [REDACTED] then told agents he also applied for unemployment benefits from Pennsylvania

1 for his wife. [REDACTED] told agents that after he received the money from Pennsylvania, he  
2 knew that it was wrong and sent the money back. [REDACTED] gave confusing and  
3 conflicting statements as to whether he had cashed the checks from Pennsylvania that  
4 were payable to [REDACTED] and [REDACTED] and whether or not he had  
5 sent that money to those individuals. [REDACTED] stated that [REDACTED] and [REDACTED] are [REDACTED]'s  
6 father and sister, respectively. He also provided conflicting statements about the  
7 MoneyGram money orders.

8 11. **COVID-19 Unemployment Benefits.** Based on publicly available  
9 information, I know that on March 27, 2020, the United States enacted into law the  
10 Coronavirus Aid, Relief, and Economic Security ("CARES") Act. The CARES Act  
11 authorized approximately \$2 trillion in aid to American workers, families, and businesses  
12 to mitigate the economic consequences of the COVID-19 pandemic. The CARES Act  
13 funded and authorized each state to administer multiple new unemployment benefits,  
14 including additional weekly payments, extension of benefits after regular benefits are  
15 exhausted, and benefits for workers who are not ordinarily eligible for unemployment  
16 benefits.

17 12. CARES Act unemployment benefits were funded by the United States  
18 government through the Department of Labor and administered at the state level by state  
19 agencies known as state workforce agencies ("SWAs").

20 13. I know from my contact with other law enforcement officers that,  
21 beginning on around April 20, 2020, officials began receiving complaints from  
22 employers about potentially fraudulent unemployment claims. The employers reported  
23 that they had received notices from SWAs indicating that persons still under their employ  
24 had filed unemployment claims. SWAs nationwide also began reporting widespread  
25 fraud and attempted fraud in connection with CARES Act unemployment benefits.

26 14. Since 2020 and in response to widespread unemployment insurance fraud  
27 related to the COVID-19 pandemic, U.S. Department of Labor, Office of Inspector  
28 General ("DOL-OIG") has maintained a database of unemployment claim data based on

1 information submitted by SWAs nationwide that are responsible for administering  
2 unemployment benefits. Among other data, the database includes the claimant's name,  
3 Social Security number, date of birth, email address, Internet Protocol ("IP") address,  
4 mailing address, and date and timestamp of application submission, bank account  
5 number, and total benefit paid.

6 15. IP address information can help to identify where computers or other  
7 devices were used to submit the application for unemployment benefits, which can also  
8 help establish who had domain over the computers or other devices that submitted the  
9 applications.

10 16. *Indicators of Fraud.* A search of the DOL-OIG database for [REDACTED]  
11 [REDACTED]'s identities yielded unemployment applications submitted to  
12 Pennsylvania from the same IP address, [REDACTED], which is located in Lancaster  
13 County, Pennsylvania. The mailing address associated with [REDACTED] and [REDACTED] is the  
14 address for SUBJECT PREMISES in Marysville, Washington, and [REDACTED]'s mailing  
15 address for her Pennsylvania claim is in Snohomish, Washington. The Snohomish  
16 address also matches the address on her and [REDACTED]'s Washington State driver's  
17 licenses, and according to the Snohomish County Assessor's website, is owned by [REDACTED]  
18 [REDACTED]. [REDACTED] is [REDACTED]'s brother, and a vehicle registered in his name  
19 was present at the SUBJECT PREMISES during the execution of Search Warrant MJ21-  
20 101.

21 17. Based on the DOL-OIG database, between May 14, 2020, and May 20,  
22 2020, the [REDACTED] IP address is associated with filing 12 applications for  
23 unemployment benefits from the Commonwealth of Pennsylvania ("Suspicious Claims"),  
24 including the claims for [REDACTED]. Only two of the mailing  
25 addresses provided for these 12 applications are within the Commonwealth of  
26 Pennsylvania. In addition to [REDACTED]'s claim, two additional claims are associated  
27 with the same mailing address in Snohomish, Washington.  
28

1 18. In response to a subpoena, Comcast provided records showing that the  
2 [REDACTED] IP address is assigned to a subscriber located at XXX [REDACTED],  
3 Lititz, Pennsylvania. One of the emails associated with the internet service account at  
4 this address is [REDACTED] and the telephone number for the account is  
5 XXX-XXX-[REDACTED]. One of the 12 claimants for the Suspicious Claims is [REDACTED],  
6 and XXX-XXX-[REDACTED] is listed as her telephone number on the application.

7 19. In or about May 2021, Pennsylvania Department of Labor and Industry  
8 ("PADOL") provided documents related to six subjects whose names were found on  
9 documents seized during the execution of Search Warrant MJ21-101, were present during  
10 the search, were referenced in [REDACTED]'s statements, and/or whose claims were  
11 associated with the Snohomish address: [REDACTED]  
12 [REDACTED]. PADOL documents show that claims were  
13 filed for these six individuals from the IP address 174.59.33.135 between May 14 and  
14 May 18, 2020. [REDACTED] claim was associated with a mailing address in Lancaster  
15 County, Pennsylvania; the five remaining claims were all associated with either the  
16 Snohomish address or the SUBJECT PREMISES. The PADOL documents showed that  
17 \$76,930 was paid for these six claims.

18 20. Based on my training and experience, I know that a common IP address  
19 associated with 12 different PADOL unemployment benefits applications that were  
20 submitted online over a one-week period means it is likely the same person or device  
21 from the same location submitted all 12 applications. [REDACTED] admitted that he  
22 applied for and received Pennsylvania unemployment benefits for three of the identified  
23 applications. Accordingly, based on my training and experience, I have probable cause to  
24 believe that [REDACTED] and/or someone he knows submitted all 12 unemployment benefit  
25 applications.

26 21. Search Warrant MJ21-101 authorized the SUBJECT FORENSIC IMAGE  
27 to be searched for stored contact information. On or about September 13, 2021, I  
28

1 searched the SUBJECT FORENSIC IMAGE and discovered contacts for 10 of the 12  
2 individuals whose names were used for the Suspicious Claims, including [REDACTED].

3 22. Search Warrant MJ21-101 also authorized the SUBJECT FORENSIC  
4 IMAGE to be searched for sent or received calls. Call logs show approximately 125 calls  
5 between [REDACTED] and [REDACTED] and hundreds of calls between [REDACTED] and  
6 at least six individuals whose names are claimants for the Suspicious Claims.

7 **BACKGROUND ON CELLULAR PHONES**

8 26. As described above and in Attachment B, this application seeks permission  
9 to search the SUBJECT FORENSIC IMAGE of the Samsung cellular phone seized at  
10 SUBJECT PREMISES. Based on my training and experience, I know that persons  
11 engaged in a conspiracy to defraud will often use cellular phones to text or otherwise  
12 communicate with their co-conspirators.

13 27. Based on my training and experience, I know that a cellular phone usually  
14 contains a "call log," which records the telephone number, date, and time of calls made to  
15 and from the phone. Cellular phones may also include global positioning system  
16 ("GPS") for determining the location of the device. A cellular phone usually also has the  
17 ability to take and store pictures as digital picture files using a built-in camera. In my  
18 training and experience, examining data stored on devices of this type can uncover,  
19 among other things, evidence that reveals or suggests who possessed or used the device  
20 and communications between the user of the device and others. Based on my knowledge,  
21 training, and experience, I know that electronic devices can store information for long  
22 periods of time.

23 28. There is probable cause to believe that things that were once stored on the  
24 Subject Device may still be stored there, for at least the following reasons:

- 25 a. Based on my knowledge, training, and experience, I know that computer  
26 files or remnants of such files can be recovered months or even years after  
27 they have been downloaded onto a storage medium, deleted, or viewed via  
28

1 the Internet. Electronic files downloaded to a storage medium can be stored  
2 for years at little or no cost. Even when files have been deleted, they can be  
3 recovered months or years later using forensic tools. This is so because  
4 when a person “deletes” a file on a computer, the data contained in the file  
5 does not actually disappear; rather, that data remains on the storage medium  
6 until it is overwritten by new data.

- 7 b. Therefore, deleted files, or remnants of deleted files, may reside in free  
8 space or slack space—that is, in space on the storage medium that is not  
9 currently being used by an active file—for long periods of time before they  
10 are overwritten. In addition, a computer’s operating system may also keep  
11 a record of deleted data in a “swap” or “recovery” file.
- 12 c. Wholly apart from user-generated files, computer storage media—in  
13 particular, computers’ internal hard drives—contain electronic evidence of  
14 how a computer has been used, what it has been used for, and who has used  
15 it. To give a few examples, this forensic evidence can take the form of  
16 operating system configurations, artifacts from operating system or  
17 application operation, file system data structures, and virtual memory  
18 “swap” or paging files. Computer users typically do not erase or delete this  
19 evidence, because special software is typically required for that task.  
20 However, it is technically possible to delete this information.
- 21 d. Similarly, files that have been viewed via the Internet are sometimes  
22 automatically downloaded into a temporary Internet directory or “cache.”

23 29. ***Forensic Evidence:*** As further described in Attachment B, this application  
24 seeks permission to locate not only electronically stored information that might serve as  
25 direct evidence of the crimes described on the warrant, but also forensic evidence that  
26 establishes how the Device was used, the purpose of its use, who used it, and when.  
27  
28

1 There is probable cause to believe that this forensic electronic evidence might be on the  
2 Device because:

3 30. Data on the storage medium can provide evidence of a file that was once on  
4 the storage medium but has since been deleted or edited, or of a deleted portion of a file  
5 (such as a paragraph that has been deleted from a word processing file).

6 31. Forensic evidence on a device can also indicate who has used or controlled  
7 the device. This “user attribution” evidence is analogous to the search for “indicia of  
8 occupancy” while executing a search warrant at a residence.

9 32. A person with appropriate familiarity with how an electronic device works  
10 may, after examining this forensic evidence in its proper context, be able to draw  
11 conclusions about how electronic devices were used, the purpose of their use, who used  
12 them, and when.

13 33. The process of identifying the exact electronically stored information on a  
14 storage medium that is necessary to draw an accurate conclusion is a dynamic process.  
15 Electronic evidence is not always data that can be merely reviewed by a review team and  
16 passed along to investigators. Whether data stored on a computer is evidence may  
17 depend on other information stored on the computer and the application of knowledge  
18 about how a computer behaves. Therefore, contextual information necessary to  
19 understand other evidence also falls within the scope of the warrant.

20 34. Further, in finding evidence of how a device was used, the purpose of its  
21 use, who used it, and when, sometimes it is necessary to establish that a particular thing is  
22 not present on a storage medium.

23 35. ***Nature of examination.*** Based on the foregoing, and consistent with Rule  
24 41(e)(2)(B), the warrant I am applying for would permit the examination of the  
25 SUBJECT FORENSIC IMAGE consistent with the warrant. The examination may  
26 require authorities to employ techniques, including but not limited to imaging or  
27 otherwise copying storage media, or using computer-assisted scans of the entire medium,  
28

1 that might expose many parts of the device to human inspection in order to determine  
2 whether it is evidence described by the warrant.

3 **CONCLUSION AND REQUEST FOR SEALING**

4 36. As set forth above, the SUBJECT FORENSIC IMAGE was seized pursuant  
5 to Search Warrant MJ21-101 for counterfeit-related offenses. However, based on  
6 evidence gathered during and after execution of Search Warrant MJ21-101, as detailed  
7 above, there is probable cause to believe that the SUBJECT FORENSIC IMAGE  
8 contains evidence, fruits and/or instrumentalities of crimes beyond the scope of  
9 Attachment B of Search Warrant MJ21-101. Accordingly, the warrant I am applying for  
10 will permit seizing evidence, fruits and/or instrumentalities of the SUBJECT  
11 OFFENSES, as specified in Attachment B of this application.

12 37. Based on the information contained herein, I request that the Court issue  
13 the proposed warrant and seal all material in support of this application. Although  
14 SHEIKH is aware of the investigation generally, premature disclosure of the warrant,  
15 affidavit, or other material may alert the targets of the scope and nature of the  
16 investigation and result in the destruction of evidence or flight of the suspects. It is  
17 respectfully requested that this Court issue an order sealing all papers submitted in  
18 support of this application, including this affidavit, the application, and search warrant  
19 until the earliest of the following: (a) two weeks following the unsealing of any charging  
20 document in a matter for which the warrants were issued; (b) two weeks following the  
21 closure of the investigation for which the warrants were issued; or (c) sixteen months

22 //

23 //

24 //

1 following issuance of the warrant, unless the Court, upon motion of the government for  
2 good cause, orders an extension of this Order.  
3  
4

5 *Robert C. Patterson*

6 \_\_\_\_\_  
7 ROBERT C. PATTERSON, Affiant  
8 Special Agent, DHS-ICE

9 The above-named agent provided a sworn statement attesting to the truth of the  
10 contents of the foregoing affidavit by telephone on the 22<sup>nd</sup> day of October, 2021.  
11

12 

13 \_\_\_\_\_  
14 MICHELLE L. PETERSON  
15 United States Magistrate Judge  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**ATTACHMENT A**

**Property to Be Searched**

The property to be searched (“SUBJECT FORENSIC IMAGE”) is the digital forensic image of the [REDACTED] cellular telephone, IMEI number [REDACTED]. Federal law enforcement agencies currently have custody of the SUBJECT FORENSIC IMAGE.

**ATTACHMENT B**

**Particular Things to be Seized**

The government is authorized to seize the following material:

For the period of March 27, 2020 to the present, the following records on the SUBJECT FORENSIC IMAGE, as described in Attachment A, that relate to violations of Title 18, United States Code, Sections 641 (Theft of Public Funds), 1341 (Mail Fraud), 1343 (Wire Fraud), 1028A (Aggravated Identity Theft), and conspiracy to commit these offenses (“SUBJECT OFFENSES”):

1. Any material mentioning, referring or relating to unemployment benefits administered by the United States or any U.S. state, including material relating to the Pennsylvania Department of Labor and Industry or any other state workforce agency;
2. Any material listing personal identifying information, including full names, Social Security numbers, addresses, phone numbers, or email addresses;
3. Any identification cards or documents, such as driver’s licenses, passports, or employment identification cards;
4. Evidence of user attribution showing who used or owned the cellular phone at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history; and
5. Evidence on the SUBJECT FORENSIC IMAGE showing the location of the phone at the time the things described in this warrant were created, edited or deleted.

This warrant authorizes a review of electronic-storage media and electronically stored information seized or copied pursuant to this warrant to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney

1 support staff, and technical experts. Pursuant to this warrant, the investigative agency  
2 may deliver a complete copy of the seized or copied electronic data to the custody and  
3 control of attorneys for the government and their support staff for their independent  
4 review.  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28